Procedimiento

Recepción, recolección y preservación de evidencias digitales

Unidad de Proyección Normativa y Estudios de Regulación Financiera

Contenido

1. Objetivo

Describir de manera detallada las actividades necesarias que permitan la recepción, recolección y preservación de las evidencias digitales generadas en desarrollo de los procesos disciplinarios adelantados en la UAE, Unidad de Proyección Normativa y Estudios de Regulación Financiera - URF, salvaguardando la confidencialidad, integridad y disponibilidad de los elementos materiales probatorios y evidencias físicas (**EMP** y **EF**[1]**)**, para que tengan plena validez legal dentro del proceso disciplinario y cualquier otra actuación judicial o jurisdiccional.

2. Alcance

Este procedimiento inicia con la recepción, adquisición, recolección y preservación de los elementos materiales probatorios y las evidencias digitales generadas en la UAE, Unidad de Proyección Normativa y Estudios de Regulación Financiera - URF o a través de la adquisición de elementos materiales probatorios y evidencias físicas halladas por fuera del desarrollo de una diligencia o audiencia, y como resultado del desarrollo normal del recaudo probatorio y el curso procesal de cada actuación disciplinaria.

Se entiende que el procedimiento finaliza, cuando las evidencias físicas y digitales y los elementos materiales probatorios, han sido recepcionados, adquiridos, recolectados, preservados y puestos a disposición ante la autoridad competente.

Este procedimiento se encuentra estructurado a partir de los lineamientos establecidos en el "Manual del Sistema de Cadena de Custodia", instrumento estandarizado por la Fiscalía General de la Nación y aplicable a todas las entidades colombianas que estén involucradas con el sistema de cadena de custodia, quienes tienen la obligación de propender por la adecuada publicación, socialización y constante actualización.

En consecuencia, se entiende incorporado a este procedimiento el "Manual del Sistema de Cadena Custodia" de la Fiscalía General de la Nación, junto con los parámetros técnicos establecidos en el Rótulo elementos materiales probatorios y evidencia física – FPJ – 7 y Formato Registro de Cadena de Custodia – FPJ-8.

[1] **EMP y EF** cualquier objeto, instrumento o medio de conocimiento conducente al descubrimiento de la verdad, como son huellas, marcas o rastros de origen físico, químico, biológico o electrónico, perceptible a través de los sentidos o mediante la utilización de tecnología forense, cuyo análisis proporciona las bases científicas o técnicas para encaminar la investigación disciplinaria o penal, lograr la identificación del autor o autores, y así confirmar o descartar la comisión de una conducta punible y la reconstrucción de los hechos.

3. Productos esperados

En ejecución del procedimiento de recepción, recolección y preservación de evidencias digitales generadas en la URF, se espera obtener los siguientes productos:

- Garantizar la autenticidad y capacidad demostrativa, de la evidencias físicas y elementos materiales probatorios hallados y recolectados por los operadores disciplinarios, en ejercicio de la potestad disciplinaria, garantizando su validez legal en el proceso disciplinario, procesos judiciales y jurisdiccionales, observando la integridad de la información y su preservación hasta su disposición final ante autoridad competente.

- Cadena de custodia de los **EMP** y **EF** recolectados.

4. Condiciones especiales del procedimiento

Las actividades de adquisición y/o recopilación de evidencia debe realizarse en cada uno de sus ciclos (recepción, adquisición y preservación) con el asesoramiento legal suficiente, de manera que se usen métodos y técnicas legalmente justificables.

Es de vital importancia mantener un procedimiento para el tratamiento de evidencia digital, el cual debe considerar las mejores prácticas existentes; sin embargo, el mismo debe ser acoplado a la realidad de la Unidad, con la finalidad de que dicha evidencia tenga valor en un proceso judicial y/o investigación interna.

4.1. Reglas de Evidencia

La evidencia digital tiene la característica de ser volátil y fácilmente manipulable, siendo vital considerar los siguientes principios (Sheetz, 2013)[2] que permiten que sea válida en los tribunales de justicia.

Existen cinco reglas que gobiernan la evidencia digital, que deben considerarse cuando se recolecta; dichos principios, permiten conocer qué se puede y no hacer cuando se trata de evidencia digital.

a) Admisible. - La evidencia debe poder ser utilizada en procesos legales.

[2] Sheetz, M. (2013). Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers. John Wiley & Sons.

b) Auténtica. - La evidencia debe ser real y relacionarse con el incidente de manera relevante.

c) Completa. - La evidencia debe ser suficiente, demostrar una perspectiva integral del incidente y poder probar las acciones o inocencia del atacante.

d) Confiable. - La evidencia que se recolecta y posteriormente se analiza, no debe causar duda de su autenticidad y veracidad; en otras palabras, contar toda la historia.

e) Creíble. - La evidencia debe ser claramente entendible y convincente para un Juez.

Como guía para el cumplimiento de los principios se han desarrollado estándares para la recolección y preservación de la evidencia digital; estos estándares han sido desarrollados por algunas organizaciones, los mismos que de manera general confluyen en:

- La evidencia original debe ser preservada en el estado más cercano al que fue encontrado.
- Las personas que ejecuten las actividades de adquisición o recopilación de la evidencia deben ser debidamente capacitadas para el efecto.
- Crear una copia exacta (imagen) de la evidencia original, la cual debe ser usada para efectuar las operaciones de análisis.
- Las copias que se realicen deben ser realizadas en medios limpios; es decir, que no exista información previa.
- Toda la evidencia debe ser etiquetada, documentada de manera apropiada y la cadena de custodia preservada. La cadena de custodia es de extrema importancia, debido a que indica: quién tiene acceso al dispositivo en cualquier momento en el tiempo, usualmente contiene los registros de bitácora de la recolección, manejo, trasporte, almacenamiento y cambios de custodio.

4.1.1. Cadena de custodia: El sistema de cadena de custodia es un proceso continuo y documentado aplicado a los EMP y EF, por parte de los servidores públicos y particulares que con ocasión a sus funciones deban garantizar su

autenticidad y capacidad demostrativa, mientras que la autoridad competente ordena su disposición final.[3]

El protocolo de cadena de custodia busca registrar de forma adecuada el manejo y almacenamiento que se da a una pieza de evidencia, este debe contener al menos:

- Fecha y hora
- Ubicación geográfica
- Nombre del cliente/oficina
- Nombre del investigador/consultor que etiqueta
- Nombre de quien realiza la adquisición de la información
- Método de adquisición / recopilación
- Estado en la que se encuentra la evidencia
- Descripción del ítem:
- HASH
- Identificador (Serial)
- Notas relevantes
- Propósito (peritaje, custodia, traslado, creación imagen, entrega al cliente, destrucción).

4.1.2. Resguardar la evidencia: Embalar y sellar la evidencia bajo condiciones adecuadas en función al tipo de evidencia, hacer uso de fundas antiestáticas, contenedores acolchados, etc.; se debe sellar el contenedor, indicando los datos de la persona que realizado dicha actividad.

4.1.3. Trasladar la evidencia: Completar la cadena de custodia, indicando: fecha y hora de entrega, nombre, cédula de identificación, firma, nombre y observaciones de quien envía y recibe. Finalmente, proceder a trasladar la evidencia.

5. Términos y definiciones

- **Diligencia:** inspección de tipo judicial que se realiza dentro de una investigación. Es toda actuación que efectúan los funcionarios públicos en ejercicio de sus respectivas atribuciones y toda actividad que realizan los particulares ante las dependencias del Estado u oficiales públicos.

- **EF (Evidencia Física):** todo elemento tangible que permite objetivar una observación y es útil para apoyar o confrontar una hipótesis.

[3] Manual de cadena de Custodia Fiscalía General de la Nación – Colombia 2018.

- **EMP (Elemento Material Probatorio):** evidencia física, objeto, instrumento o producto relacionado con un hecho delictivo y que puede constituirse como prueba.

- **La Evidencia informática:** se constituye por datos de valor investigativo almacenados o transmitidos por un computador.

6. Definición del procedimiento

No.	Actividad	PC	Responsable	Explicación	Registro
A. Recepción de audiencias y/o diligencias en la sala de audiencias de la OCDI					
1.	Descargar el audio y video de la diligencia o audiencia.		Servidor designado	Consiste en revisar el contenido completo de la diligencia y/o audiencia, y descargar su contenido directamente en un dispositivo de almacenamiento CD'S o DVD'S.	CD'S o DVD'S
2.	Descargar los metadatos de los contenidos descargados.		Servidor designado	Incorporar dentro del dispositivo de almacenamiento CD'S o DVD'S un archivo en donde se identifiquen los metadatos asociados a la diligencia y/o audiencia.	CD'S o DVD'S
3.	Diligenciar formato de identificación de metadatos y registro de códigos		Servidor designado	Registrar de forma adecuada, todos los ítems asociados al manejo y almacenamiento que se encuentra en el formato de identificación de metadatos y registro de códigos.	Formato de identificación de metadatos y registro de código.
4.	Anexar al expediente físico y virtual.		Servidor designado	Incorporar según secuencia documental y flujo de expediente virtual, los siguientes documentos: 1) Contenido de audio y video de la diligencia o audiencia y 2) formato de identificación de metadatos y registro de códigos.	Expediente físico y expediente virtual SIED.
B. Recepción de documentos en dispositivos de almacenamiento electrónicos					

No.	Actividad	PC	Responsable	Explicación	Registro
5.	Identificar el contenido del Documento y su medio de almacenamiento.	[redacted]	Servidor designado	Consiste en efectuar un correcto control y filtro al contenido guardado en los diversos dispositivos de almacenamiento; lo anterior, con el fin de determinar la fiabilidad y toda la información relacionada con el receptor de la información, que en este caso se conoce como el que "halló" la EF y/o EMP.	USB, CD'S o DVD's.
6.	Descargar los metadatos y obtener códigos del aplicativo institucional.		Servidor designado	Incorporar dentro del dispositivo de almacenamiento CD'S o DVD'S un archivo en donde se identifiquen los metadatos y códigos asociado a la EF o EMP allegado.	USB, CD'S o DVD's
7.	Diligenciar formato de rótulo elemento de prueba o evidencia física.		Servidor designado	Registrar de forma adecuada, todos los ítems asociados al manejo y almacenamiento que se encuentra en el formato de rótulo elementos de prueba o evidencia física.	Formato de rótulo elemento de prueba o evidencia física.
8.	Diligenciamiento del formato de cadena de custodia	[redacted]	Servidor designado	Registrar de forma adecuada, todos los ítems asociados al formato de cadena de custodia y hacer seguimiento constante al mismo.	Formato de cadena de custodia
9.	Anexar al expediente físico y virtual.		Servidor designado	Incorporar según secuencia documental y flujo de expediente virtual, los siguientes documentos: 1) Contenido del medio de almacenamiento allegado y 2) Formato de rotulo elemento de prueba o evidencia física y 3) Formato de cadena de custodia.	Expediente físico y expediente virtual SIED.
Recolección de evidencias físicas y elementos materiales probatorios.					

No.	Actividad	PC	Responsable	Explicación	Registro
10.	Identificar los EMP y EF, susceptibles de ser recopilados.		Servidor designado	Consiste en definir: **1)** El lugar donde se hallan las evidencias físicas o elementos materiales probatorios, **2)** identificar el custodio de la información, donde se encuentra contenida las mismas, **3)** si se trata de evidencias digitales o elementos físicos y **4)** Donde se van a recaudar los elementos**.5)** informar al custodio de la información y **6)** Comunicar al investigado.	Auto decreta pruebas de oficio.
11.	Programar y realizar diligencia y/o audiencia de recolección y legalización de EMP y EF.		Servidor designado	Conforme al procedimiento ordinario o verbal, en el sitio donde se halla la EF o el EMP y en presencia del custodió de la información y/o el investigado si este compareciere, se protocoliza el recaudo de los elementos a través de diligencia de recolección y legalización de EMP Y EF.	Diligencia y/o audiencia de recolección y legalización de EMP y EF.
12.	Diligenciar formato de rotulo elemento de prueba o evidencia física.	[redacted]	Servidor designado	Registrar de forma adecuada, todos los ítems asociados al manejo y almacenamiento que se encuentra en el formato de rotulo elementos de prueba o evidencia física.	Formato de rotulo elemento de prueba o evidencia física.
13.	Anexar al expediente físico y virtual		Servidor designado	Incorporar según secuencia documental y flujo de expediente virtual, los siguientes documentos: 1) Contenido del medio de almacenamiento recaudado o fotos del elemento físico, 2) Formato de rotulo elemento de prueba o evidencia física y 3) Formato de cadena de custodia.	Expediente físico y expediente virtual SIED.
Fin del procedimiento					

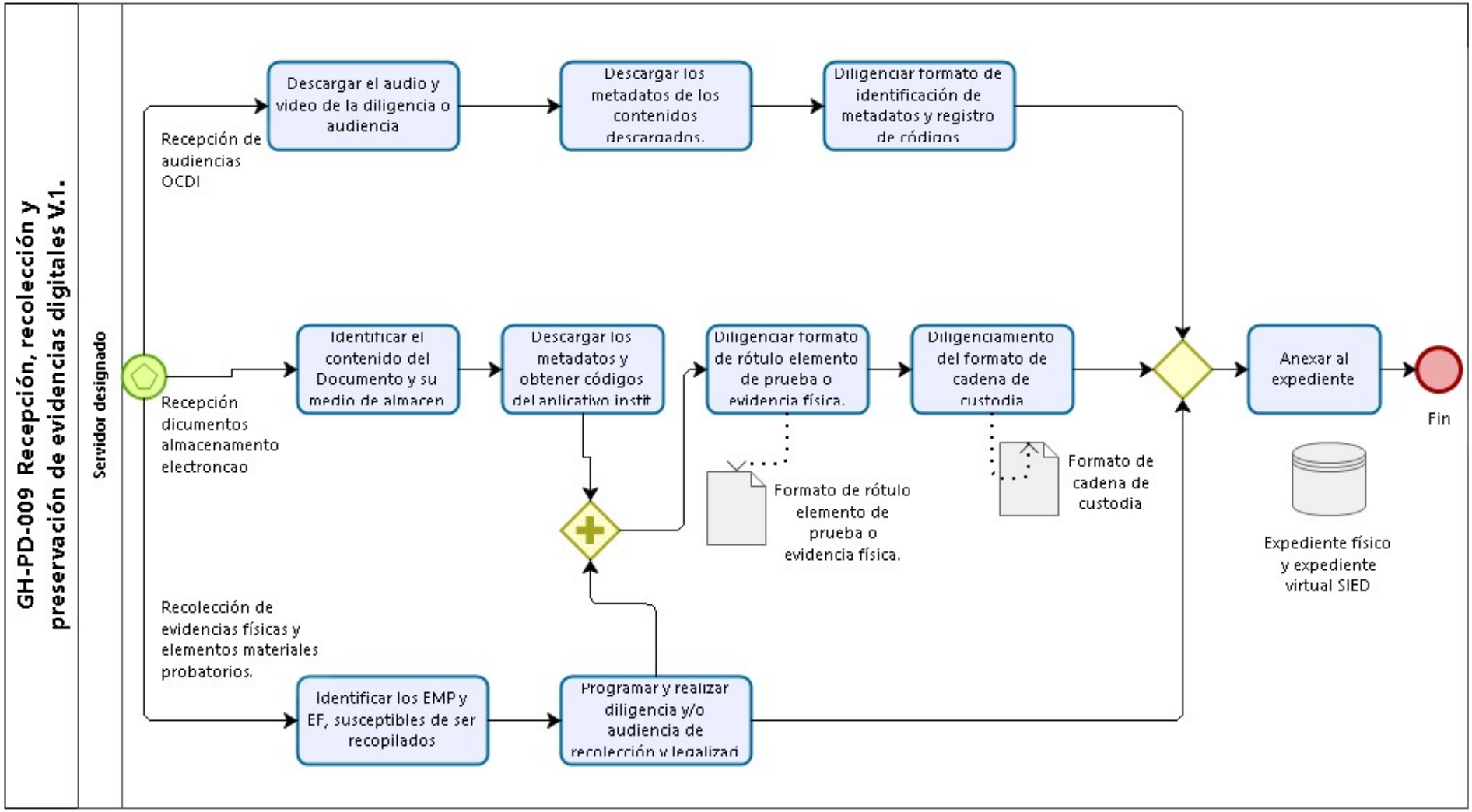
7. Documento referente

Tipo	Nombre
Caracterización	Caracterización proceso Gestión Humana

8. Datos de elaboración y control de cambios

Control de cambios			
Fecha	**Versión**	**Cód. Solicitud**	**Descripción del cambio**
2024-04-15	1.0	TS-0461	Creación del documento

Elaboración, revisión y aprobación	
Elaboración	
Nombre:	Catalina Torrado Ulloa
Cargo:	Profesional Especializado
Revisión	
Nombre:	Kevin Steven Correa Fajardo
Cargo:	Asesor Líder Proceso de Gestión Humana
Aprobación	
Nombre:	Paola Patricia Rodríguez Angulo
Cargo:	Subdirectora Jurídica y de Gestión Institucional


GH-PD-009 Recepción, recolección y preservación de evidencias digitales V.1.
Servidor designado
Descargar el audio y video de la diligencia o audiencia
Descargar los metadatos de los contenidos descargados.
Diligenciar formato de identificación de metadatos y registro de códigos
Recepción de audiencias OCDI
Identificar el contenido del Documento y su medio de almacen
Descargar los metadatos y obtener códigos del aplicativo instit
Diligenciar formato de rótulo elemento de prueba o evidencia física.
Diligenciamiento del formato de cadena de custodia
Anexar al expediente
Fin
Recepción dicumentos almacenamento electroncao
Formato de rótulo elemento de prueba o evidencia física.
Formato de cadena de custodia
Expediente físico y expediente virtual SIED
Recolección de evidencias físicas y elementos materiales probatorios.
Identificar los EMP y EF, susceptibles de ser recopilados
Programar y realizar diligencia y/o audiencia de recolección y legalizad